

CLAIM AMENDMENTS

1. (currently amended) Apparatus for facilitating digital signing of electronic data, said ~~system~~ apparatus comprising:
 - a browser;
 - coupled to the browser, a signing module; and
 - coupled to the browser and to the signing module, a signing interface, the signing interface adapted to be invoked by an executable software program transmitted to the browser from a remote location, and to:
 - forward data to be signed to the signing module,
 - receive a digital signature for the data to be signed from the signing module, and
 - forward the digital signature to the remote location;
 - wherein the signing interface comprises a signing plug-in and a signing interface library having an API.
2. (previously presented) The apparatus of claim 1, wherein the signing interface comprises a signing interface library having an API, and the executable software program is an applet referenced in a Web page transmitted to the browser from a Web server.
3. (previously presented) The apparatus of claim 2, wherein the applet is adapted to retrieve the data to be signed from a remote location and to forward the data to be signed to the signing interface.
4. (previously presented) The apparatus of claim 2, wherein the applet is digitally signed.
5. (previously presented) The apparatus of claim 1, wherein the signing interface comprises a signing plug-in and the executable software program comprises a Web page comprising a tag adapted to launch the signing plug-in.
6. (previously presented) The apparatus of claim 5, wherein the tag is an `<EMBED>` tag.

7. (previously presented) The apparatus of claim 5, wherein the tag is an <OBJECT> tag.
8. (previously presented) The apparatus of claim 1, wherein the data to be signed is retrieved from a remote location specified by the executable software program.
9. (previously presented) The apparatus of claim 1, wherein the data to be signed is included in the executable software program.
10. (previously presented) The apparatus of claim 1, wherein the signing module digitally signs the data to be signed with an identity key.
11. (previously presented) The apparatus of claim 1, wherein the signing module is a smart card subsystem.
12. (previously presented) The apparatus of claim 1, wherein the digitally signed data includes card and signature security data.
13. (previously presented) The apparatus of claim 1, wherein the signing interface is obtained from a trusted entity.
14. (previously presented) The apparatus of claim 13, wherein the signing interface is digitally signed by the trusted entity.
15. (previously presented) The apparatus of claim 14, wherein the trusted entity is an issuing financial institution.
16. (previously presented) The apparatus of claim 1, wherein the signing interface comprises a user interface.
17. (previously presented) The apparatus of claim 16, wherein the user interface displays the data to be signed to a user, and, prior to the signing interface obtaining the digital signature from the signing module, obtains the user's approval to sign the data.
18. (previously presented) The apparatus of claim 16, wherein the user interface offers a user an opportunity to store the data to be signed.

19. (previously presented) The apparatus of claim 16, wherein the user interface offers a user an opportunity to view the data to be signed in a software application.
20. (previously presented) The apparatus of claim 19, wherein the software application is a spreadsheet.
21. (currently amended) A method for facilitating digital signing of electronic data, said method comprising the steps of:
- a browser receiving an executable software program from a remote location;
 - the executable software program triggering a signing interface, coupled to the browser, to forward data to be signed to a signing module;
 - the signing module sending to the signing interface a digital signature for the data to be signed; and
 - the signing interface forwarding the digital signature to [[a]] the remote location;
- wherein the signing interface comprises a signing plug-in and a signing interface library having an API.
22. (previously presented) The method of claim 21, wherein the signing interface comprises a signing interface library having an API and the executable software program is an applet referenced in a Web page transmitted to the browser from a Web server.
23. (original) The method of claim 22, wherein the applet is adapted to retrieve the data to be signed from a remote location and to forward the data to be signed to the signing interface.
24. (original) The method of claim 22, wherein the applet is digitally signed.
25. (previously presented) The method of claim 21, wherein the signing interface comprises a signing plug-in and the executable software application comprises a Web page comprising a tag adapted to launch the signing plug-in.
26. (original) The method of claim 25, wherein the tag is an <EMBED> tag.
27. (original) The method of claim 25, wherein the tag is an <OBJECT> tag.

28. (previously presented) The method of claim 21, wherein the data to be signed is retrieved from a remote location specified by the executable software program.
29. (previously presented) The method of claim 21, wherein the data to be signed is included in the executable software program.
30. (original) The method of claim 21, wherein the signing module digitally signs the data to be signed with an identity key.
31. (original) The method of claim 21, wherein the signing module is a smart card subsystem.
32. (original) The method of claim 21, wherein the digitally signed data includes card and signature security data.
33. (original) The method of claim 21, wherein the signing interface is obtained from a trusted entity.
34. (original) The method of claim 33, wherein the signing interface is digitally signed by the trusted entity.
35. (previously presented) The method of claim 34, wherein the trusted entity is an issuing financial institution.
36. (original) The method of claim 21, wherein the signing interface comprises a user interface.
37. (previously presented) The method of claim 36, wherein, prior to the step of the signing module sending to the signing interface a digital signature, the user interface displays the data to be signed to a user and obtains the user's approval to sign the data.
38. (original) The method of claim 36, wherein the user interface offers a user the opportunity to store the data to be signed.
39. (previously presented) The method of claim 36, wherein the user interface offers a user an opportunity to view the data to be signed in a software application.

40. (original) The method of claim 39, wherein the software application is a spreadsheet.

41. (currently amended) Apparatus for facilitating digitally signing data by a first customer, said ~~system~~ apparatus comprising:

- a browser;

- coupled to the browser, a signing module;

- coupled to the browser and to the signing module, a signing interface, the signing interface being adapted to facilitate access to system services provided via a four-corner model comprising a root entity, a first financial institution, a second financial institution, the first customer, and a second customer, the second customer maintaining a second-customer computer system;

- coupled to the browser, means for downloading an executable software program from the second-customer computer system to the browser;

- coupled to the downloading means, means for invoking the signing interface;

- coupled to the invoking means, means for determining whether to request a system service;

- coupled to the determining means, means for creating a service request for the system service;

- coupled to the creating means, means for transmitting the service request;

- coupled to the transmitting means, means for receiving a response to the service request;

- coupled to the means for receiving a response, means for forwarding the data to be signed to the signing module;

- coupled to the forwarding means, means for receiving a digital signature for the data to be signed from the signing module; and

- coupled to the means for receiving a digital signature, means for forwarding the digital signature to a remote location specified by the executable software program;

- wherein the signing interface comprises a signing plug-in and a signing interface library having an API.

42. (previously presented) The apparatus of claim 41, wherein the determining means comprises means for presenting to the first customer an option to request a system service.

43. (previously presented) The apparatus of claim 42, wherein the system service is a warranty.

44. (previously presented) The apparatus of claim 43, wherein the response to the service request comprises a warranty and the warranty is forwarded with the digital signature to the remote location specified by the executable software program.

45. (previously presented) A method for accessing system services provided via a four-corner model, the four corner model comprising:

- a root entity;

- a first financial institution;

- a second financial institution;

- a first customer, said first customer being a customer of the first financial institution, said first customer maintaining a first-customer computer system, said first-customer computer system comprising:

- a browser,

- a signing module,

- and a signing interface; and

- a second customer, said second customer being a customer of the second financial institution, said second customer maintaining a second-customer computer system, said second-customer computer system comprising a Web server adapted to send an executable computer program to the first-customer computer system's browser, the method comprising the steps of:

- invoking the signing interface;

- retrieving data to be signed from a remote location;

- determining whether to request a system service;

- creating a service request for the system service;

- transmitting the service request;

receiving a response to the service request;
forwarding the data to be signed to the signing module;
receiving a digital signature for the data to be signed from the signing module;
and
forwarding the digital signature to the remote location;
wherein the signing interface comprises a signing plug-in and a signing interface library having an API.

46. (previously presented) The method of claim 45, further comprising the step of presenting to the first customer an option to request a system service.

47. (previously presented) The method of claim 46, wherein the system service is a warranty.

48. (previously presented) The method of claim 45, wherein the response to the service request comprises a warranty and the warranty is forwarded with the digital signature to the remote location.